





Franking system for postal handling has network coupled computer with built in security module

Publication number: DE10055145
Publication date: 2002-05-16
Inventor: LANG JUERGEN (DE); MEYER BERND (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
- international: **G07B17/00; G07B17/00; (IPC1-7): G07B17/02**
- european: G07B17/00D2
Application number: DE20001055145 20001107
Priority number(s): DE20001055145 20001107

Also published as:

 W 00239390 (A1)
 US 2005278265 (A1)
 E P1340197 (A0)
 CA 2428298 (A1)

[Report a data error here](#)

Abstract of DE10055145

The postal franking system for a customer is based around a personal computer that is linked by a server and network to a central station that handles franking values. Built into the customer's computer system is a security module that prevents misuse of the franking process.

Data supplied from the esp@cenet database - Worldwide



⑮ **BUNDESREPUBLIK
DEUTSCHLAND**



**DEUTSCHES
PATENT- UND
MARKENAMT**

⑫ **Offenlegungsschrift**
⑩ **DE 100 55 145 A 1**

⑤① Int. Cl.7:
G 07 B 17/02

⑲ Aktenzeichen: 100 55 145.9
⑳ Anmeldetag: 7. 11. 2000
㉑ Offenlegungstag: 16. 5. 2002

DE 100 55 145 A 1

⑦① Anmelder:
Deutsche Post AG, 53175 Bonn, DE

⑦④ Vertreter:
Jostarndt, H., Dipl.-Phys. Dr.rer.nat., Pat.-Anw.,
52074 Aachen

⑦② Erfinder:
Lang, Jürgen, Dr., 51429 Bergisch Gladbach, DE;
Meyer, Bernd, 53639 Königswinter, DE

⑤⑥ Entgegenhaltungen:
DE 198 12 903 A1
DE 197 37 232 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤④ Verfahren zum Versehen von Postsendungen mit Frankierungsvermerken

⑤⑦ Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Frankierungsvermerken, wobei ein Kundensystem ein Drucken von Frankiervermerken auf Postsendungen steuert.
Erfindungsgemäß wird das Verfahren so durchgeführt, dass in einer Datei erfasst wird, für welche durch einen Druckbefehl erzeugte Frankiervermerke keine Versendung einer Postsendung erfolgt.

DE 100 55 145 A 1

[0001] Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Frankierungsvermerken, wobei ein Kundensystem ein Drucken von Frankierungsvermerken auf Postsendungen steuert.

[0002] Es ist bekannt, eine Frankierung durch Wiedergabe von digitalisierten Daten in verschlüsselter Form zu erzeugen. Dieses Verfahren wird wegen seiner bevorzugten Durchführung auf Personal Computer nachfolgend zusammenfassend kurz als PC-Frankierung bezeichnet. Die Bezeichnung PC-Frankierung ist jedoch in keiner Weise einschränkend zu verstehen, da die Erzeugung von digitalen Daten an beliebigen Computern erfolgen kann und nicht auf Personal Computer beschränkt ist. Der Begriff "Computer" ist in keiner Weise einschränkend zu verstehen. Es handelt sich hierbei um eine beliebige, zur Durchführung von Berechnungen geeignete Einheit, beispielsweise eine Workstation, einen Personal Computer, einen Micro Computer oder eine zur Durchführung von Berechnungen geeignete Schaltung. Beispielsweise kann es sich auch um einen persönlichen digitalen Assistenten (PDA) handeln.

[0003] Eine Darstellung des von der Deutschen Post AG geplanten Frankierungsverfahrens wurde der Öffentlichkeit durch Veröffentlichung im Internet zugänglich gemacht.

[0004] Die vorgestellte PC-Frankierung enthält mehrere Schritte, in denen ein Kunde einen Portobetrag lädt, aus dem Portobetrag Frankiervermerke erzeugt und auf einem Drucker ausdruckt. Der Ausdruck erfolgt in Form eines PC-Frankiervermerks, der einen maschinenlesbaren, zweidimensionalen Matrixcode enthält, der zur Prüfung der Gültigkeit des Frankiervermerks herangezogen werden kann.

[0005] Die mit dem PC-Frankiervermerk versehene Sendung kann bei dem Postdienstleister eingeliefert werden. Der Postdienstleister befördert die Sendung nach Überprüfung der Gültigkeit des Frankiervermerks.

[0006] Um eine missbräuchliche Erzeugung von Frankiervermerken zu verhindern, erfolgt eine Verringerung des zur Verfügung stehenden Portobetrages, sobald ein entsprechender Druckbefehl ausgelöst wurde.

[0007] Es besteht hierbei das Problem, dass nach Ausgabe des Druckbefehls, jedoch vor dem tatsächlichen Ausdruck des Frankierungsvermerks die Druckdaten verloren gehen könnten. Dies kann beispielsweise bei einem Systemabsturz, einem Stromausfall, bei Papierstaus oder bei einem Ausdruck mit einer leeren Tintenpatrone oder leerer Tonerkassette erfolgen.

[0008] Der Erfindung liegt die Aufgabe zugrunde, ein gattungsgemäßes Verfahren so weiterzuentwickeln, dass eine Belastung des Benutzers mit Gebührenbeträgen über nicht zur Versendung von Postsendungen verwendete Frankiervermerke vermieden wird.

[0009] Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass in einer Datei erfasst wird, für welche durch einen Druckbefehl erzeugte Frankiervermerke keine Versendung einer Postsendung erfolgt.

[0010] Eine besonders einfache Erstattung von Gebührenbeträgen ist dadurch möglich, dass die Datei in ein Gebührenerstattungsformular übernommen wird.

[0011] Zweckmäßigerweise wird das Verfahren so durchgeführt, dass die Datei und/oder das Gebührenerstattungsformular an eine Erstattungsstelle übermittelt werden.

[0012] Zur Erhöhung der Datensicherheit ist es vorteilhaft, dass die Übermittlung an einen Server erfolgt, und dass das Kundensystem Identifikationsdaten über die nicht zu versendenden Sendungen an den Server übermittelt, und dass der Server die Identifikationsdaten an wenigstens eine Überprüfungsstelle weiterleitet.

[0013] Bei dem Server handelt es sich vorzugsweise um einen logischen Knoten eines Kommunikationsnetzwerkes, jedoch kann auch ein sonstiger mit Schnittstellen ausgestatteter Computer, beziehungsweise eine sonstige Berechnungseinheit, als Server verwendet werden.

[0014] Durch die Übermittlung der Identifikationsdaten wird ein Missbrauch der automatisierten Erstattungsmöglichkeit vermieden. Überprüfungsstellen, die vorteilhafterweise in Briefzentren angeordnet sind, die jedoch auch außerhalb der Briefzentren, beispielsweise an einer oder mehreren zentralen Stellen, zusammengefasst sind, können eine Sendung, die eingeliefert wurde, obwohl der zu ihrer Erzeugung verwendete Freimachungsvermerk von dem Kundensystem als nicht versandt markiert wurde, erkennen.

[0015] Daher ist es möglich, dass die Datei, beziehungsweise das Gebührenerstattungsformular unverschlüsselt in dem Kundensystem gespeichert werden. Eine missbräuchliche Eingabe von Angaben über nicht zur Versendung von Postsendungen verwendete Frankierwerte kann durch Ausortierung solcher Sendungen, zu denen die Briefzentren eine Nachricht erhalten haben, dass sie als Nichtversand gelten, entdeckt werden.

[0016] Auch eine manuelle Eingabe von Sendungsdaten kann von dem System zugelassen werden, da ein Missbrauch dieser manuellen Eingabemöglichkeit vermieden werden kann.

[0017] Beispielsweise kann der Benutzer des Kundensystems manuell Daten über nicht versandte Sendungen eingeben. Eine derartige manuelle Eingabe kann wahlweise – beispielsweise durch Einführung einer Verschlüsselung – ausgeschlossen oder zugelassen werden. In dem Fall, dass eine manuelle Dateneingabe zugelassen ist, kann der Benutzer des Kundensystems beispielsweise einen mit einem Frankiervermerk gekennzeichneten Briefbogen vor einer Versendung entnehmen, beispielsweise, wenn er nachträglich beschlossen hat, den mit dem Frankiervermerk gekennzeichneten Briefbogen nicht zu versenden.

[0018] Eine weitere Erhöhung der Datensicherheit ist dadurch möglich, dass eine Gebührenerstattung nur erfolgt, wenn dem Formular über die zu erstattenden Frankiervermerke Belege über den Nichtversand oder den Nichtausdruck beigelegt werden.

[0019] Diese Belege werden beispielsweise von dem System automatisiert erstellt, beispielsweise durch ein Scannen der betreffenden Frankiervermerke oder durch Protokollierung von Systemdaten über das Nichtausdrucken des Frankiervermerks.

[0020] Eine elektronische Speicherung dieser Angaben ist besonders vorteilhaft, weil so eine automatisierte Überprüfung ermöglicht wird.

[0021] Vorzugsweise erfolgt der Versand elektronisch, beispielsweise durch eine Nachricht in einem Kommunikationssystem, eine e-mail oder durch Eingabe in eine Webseite.

[0022] Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnungen.

[0023] Von den Zeichnungen zeigt

[0024] Fig. 1 ein Kundensystem zur Erzeugung von Freimachungsvermerken;

[0025] Fig. 2 ein Gesamtsystem aus einem Kundensystem und einem externen Server und

[0026] Fig. 3 eine Bildschirmmaske, welche Informationen über die nicht versandte Sendung enthält.

[0027] Das in Fig. 1 dargestellte Kundensystem umfasst beispielsweise einen Personal Computer 1 mit einem Bildschirm 2, einer Tastatur 3, einer Maus 4 und einem ange-

geschlossenen Drucker 5.

[0028] Das Kundensystem ist nicht von der dargestellten Hardware abhängig, sondern kann vielfältige materielle Formen aufweisen, beispielsweise kann es in einem einzelnen Speichermodul, beispielsweise einer Chip-Karte, gespeichert sein. 5

[0029] Bei dem in Fig. 2 dargestellten Gesamtsystem befindet sich das Kundensystem in Kontakt mit einem externen Server. Vorteilhafterweise wird der externe Server durch ein Ladezentrum (Wertübertragungszentrum) gebildet. 10

[0030] Bei dem Server kann es sich um einen beliebigen Computer handeln. Die Bezeichnung Server hat keine einschränkende Bedeutung, sondern verweist auf die zusätzliche Möglichkeit, Daten gezielt über Schnittstellen auszutauschen. 15

[0031] Eine der Schnittstellen wird vorzugsweise durch das Kundensystem bereitgestellt. Diese Schnittstelle, die nachfolgend als Kundenschnittstelle bezeichnet wird, erlaubt eine Eingabe von Daten über elektronisch erzeugte, jedoch nicht zum Versand von Postwertzeichen benutzte, Frankiervermerke. 20

[0032] Vorzugsweise enthält das Kundensystem ein Sicherungsmodul, das eine fälschungssichere Erzeugung von Frankiervermerken ermöglicht.

[0033] Das Kundensystem ist vorzugsweise Teil eines Gesamtsystems, das in allen Bestandteilen Überprüfungs- und Sicherheitsmechanismen enthält. 25

[0034] Ein weiterer Bestandteil des Gesamtsystems ist beispielsweise ein Wertübertragungszentrum. Die Eigenschaften des Wertübertragungszentrums, die ein unberechtigtes Laden von Abrechnungsbeträgen verhindern, sind nicht dargestellt, da das Kundensystem mit einem beliebigen derart gesicherten Wertübertragungszentrum verbunden werden kann. 30

Sicherheitsarchitektur

[0035] Für die PC-Frankierung ist eine grundsätzliche Sicherheitsarchitektur vorgesehen, die die Vorteile verschiedener, bestehender Ansätze verbindet und mit einfachen Mitteln ein höheres Maß an Sicherheit bietet. 40

[0036] Die Sicherheitsarchitektur umfasst vorzugsweise im Wesentlichen drei Einheiten, die in einer bevorzugten Anordnung in Fig. 2 dargestellt sind: 45

- Ein Wertübertragungszentrum, in dem die Identität des Kunden und seines Kundensystems bekannt ist.
- Ein Sicherungsmodul, das die als nicht durch den Kunden manipulierbare Hard-/Software die Sicherheit im Kundensystem gewährleistet (z. B. Dongle oder Chipkarte bei Offline-Lösungen bzw. gleichwertige Server bei Online-Lösungen).
- Ein Briefzentrum, in dem die Gültigkeit der Freimachungsvermerke geprüft, beziehungsweise Manipulationen am Wertbetrag sowie am Freimachungsvermerk erkannt werden. 55

[0037] Die einzelnen Prozessschritte, die im Wertübertragungszentrum, Kundensystem und Briefzentrum erfolgen, sollen im Folgenden in Form einer Prinzipskizze dargestellt werden. Der genaue technische Kommunikationsprozess weicht hingegen von dieser prinzipiellen Darstellung ab (z. B. mehrere Kommunikationsschritte zur Erlangung einer hier dargestellten Übertragung). Insbesondere wird in dieser Darstellung eine vertrauliche und integre Kommunikation zwischen identifizierten und authentisierten Kommunikationspartnern vorausgesetzt. 60 65

Kundensystem

1. Innerhalb des Sicherungsmoduls wird eine Zufallszahl erzeugt und zwischengespeichert, die dem Kunden nicht zur Kenntnis gelangt.

2. Innerhalb des Sicherungsmoduls wird die Zufallszahl zusammen mit einer eindeutigen Identifikationsnummer (Sicherungsmodul-ID) des Kundensystems, beziehungsweise des Sicherungsmoduls, derart kombiniert und verschlüsselt, dass nur das Wertübertragungszentrum in der Lage ist, eine Entschlüsselung durchzuführen.

In einer besonders bevorzugten Ausführungsform wird die Zufallszahl zusammen mit einem zuvor vom Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und den Nutzdaten der Kommunikation (Beantragung der Einrichtung eines Abrechnungsbetrages) mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt und mit dem privaten Schlüssel des Sicherungsmoduls digital signiert. Hierdurch wird vermieden, dass die Anfrage bei jedem Laden eines Abrechnungsbetrages dieselbe Gestalt hat und zum missbräuchlichen Laden von Abrechnungsbeträgen herangezogen werden kann (Replay-Attack).

3. Die kryptographisch behandelten Informationen aus dem Kundensystem werden an das Wertübertragungszentrum im Rahmen des Ladens eines Abrechnungsbetrages übertragen. Weder der Kunde noch Dritte können diese Informationen entschlüsseln.

[0038] In der Praxis wird die asymmetrische Verschlüsselung mit dem öffentlichen Schlüssel des Kommunikationspartners (Wertübertragungszentrum, beziehungsweise Sicherungsmodul) angewandt.

[0039] Bei der Möglichkeit eines vorhergehenden Austausches von Schlüsseln kommt eine symmetrische Verschlüsselung gleichfalls in Betracht. 35

Wertübertragungszentrum

4. Im Wertübertragungszentrum wird unter anderem die Zufallszahl, die der Identifikationsnummer des Sicherungsmoduls (Sicherungsmodul-ID) zugeordnet werden kann, entschlüsselt.

5. Durch Anfrage in der Datenbank-Freimachung wird die Sicherungsmodul-ID einem Kunden der Deutschen Post zugeordnet.

6. Im Wertübertragungszentrum wird eine Ladevorgangsidentifikationsnummer gebildet, die Teile der Sicherungsmodul-ID, die Höhe eines Abrechnungsbetrages etc. beinhaltet. Die entschlüsselte Zufallszahl wird zusammen mit der Ladevorgangsidentifikationsnummer derart verschlüsselt, dass nur das Briefzentrum in der Lage ist, eine Entschlüsselung durchzuführen. Der Kunde ist hingegen nicht in der Lage, diese Informationen zu entschlüsseln. (Die Ladevorgangsidentifikationsnummer wird zusätzlich in einer vom Kundensystem entschlüsselbaren Form verschlüsselt). In der Praxis erfolgt die Verschlüsselung mit einem symmetrischen Schlüssel nach TDES, der ausschließlich im Wertübertragungszentrum sowie in den Briefzentren vorhanden ist. Die Verwendung der symmetrischen Verschlüsselung an dieser Stelle ist begründet durch die Forderung nach schnellen Entschlüsselungsverfahren durch die Produktion.

7. Die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer werden an das Kundensystem übertragen. Weder der Kunde noch

Dritte können diese Informationen entschlüsseln. Durch die alleinige Verwaltung des posteigenen, vorzugsweise symmetrischen Schlüssels im Wertübertragungszentrum und in den Briefzentren kann der Schlüssel jederzeit ausgetauscht und Schlüssellängen können bei Bedarf geändert werden. Hierdurch wird auf einfache Weise eine hohe Manipulationssicherheit gewährleistet. In der Praxis wird die Ladevorgangsidentifikationsnummer dem Kunden zusätzlich in nicht verschlüsselter Form zur Verfügung gestellt.

Kundensystem

8. Der Kunde erfasst im Rahmen der Erstellung eines Freimachungsvermerks die sendungsspezifischen Informationen oder Sendungsdaten (z. B. Porto, Sendungsart etc.), die in das Sicherungsmodul übertragen werden.

9. Innerhalb des Sicherungsmoduls wird ein Hash-Wert unter anderem aus folgenden Informationen gebildet

- Auszügen aus den Sendungsdaten (z. B. Porto, Sendungsart, Datum, PLZ etc.),
- der zwischengespeicherten Zufallszahl (die im Rahmen des Ladens eines Abrechnungsbetrages erzeugt wurde)
- und gegebenenfalls der Ladevorgangsidentifikationsnummer.

10. In den Freimachungsvermerk werden unter anderem folgende Daten übernommen:

- Auszüge aus den Sendungsdaten im Klartext (z. B. Porto, Sendungsart, Datum, PLZ etc.),
- die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer aus dem Wertübertragungszentrum und
- der innerhalb des Sicherungsmoduls gebildete Hash-Wert aus Sendungsdaten, Zufallszahl und Ladevorgangsidentifikationsnummer.

Briefzentrum

11. Im Briefzentrum werden zunächst die Sendungsdaten geprüft. Stimmen die in den Freimachungsvermerk übernommenen Sendungsdaten nicht mit der Sendung überein, so liegen entweder eine Falschfrankierung, eine Phantasie- oder eine Schmiermarke vor. Die Sendung ist der Entgeltsicherung zuzuführen.

12. Im Briefzentrum werden die Zufallszahl und die Ladevorgangsidentifikationsnummer, die im Rahmen des Abrechnungsbetrages an das Kundensystem übergeben wurden, entschlüsselt. Hierzu ist im Briefzentrum nur ein einziger (symmetrischer) Schlüssel erforderlich. Bei Verwendung von individuellen Schlüsseln wäre jedoch statt dessen eine Vielzahl von Schlüsseln einzusetzen.

13. Im Briefzentrum wird nach demselben Verfahren wie in dem Sicherungsmodul ein Hash-Wert aus folgenden Informationen gebildet:

- Auszügen aus den Sendungsdaten,
- der entschlüsselten Zufallszahl
- der entschlüsselten Ladevorgangsidentifikationsnummer.

14. Im Briefzentrum werden der selbstgebildete und der übertragene Hash-Wert verglichen. Stimmen beide überein, so wurde der übertragene Hash-Wert mit derselben Zufallszahl gebildet, die auch dem Wertübertragungszentrum im Rahmen des Ladens des Abrechnungsbetrages übermittelt wurde. Demnach handelt es

sich sowohl um einen echten, gültigen Abrechnungsbetrag als auch um Sendungsdaten, die dem Sicherungsmodul bekanntgegeben wurden (Gültigkeitsprüfung). Vom Aufwand her entsprechen die Entschlüsselung, die Bildung eines Hash-Wertes und der Vergleich von zwei Hash-Werten theoretisch dem einer Signaturprüfung. Aufgrund der symmetrischen Entschlüsselung entsteht jedoch gegenüber der Signaturprüfung ein zeitlicher Vorteil.

15. Über eine Gegenprüfung im Hintergrundsystem können im Nachhinein Abweichungen zwischen geladenen Abrechnungsbeträgen und Frankierbeträgen ermittelt werden (Überprüfung hinsichtlich Sendungsdubletten, Saldenbildung im Hintergrundsystem).

[0040] Die dargestellte grundsätzliche Sicherheitsarchitektur umfasst nicht die separat abgesicherte Verwaltung der Abrechnungsbeträge (Börsenfunktion), die Absicherung der Kommunikation zwischen Kundensystem und dem Wertübertragungszentrum, die gegenseitige Identifizierung von Kundensystem und Wertübertragungszentrum und die Initialisierung zur sicheren Betriebsaufnahme eines neuen Kundensystems.

Angriffe auf die Sicherheitsarchitektur

[0041] Die beschriebene Sicherheitsarchitektur ist sicher gegenüber Angriffen durch Folgendes:

– Dritte können die im Internet mitgeschnittene (kopierte) erfolgreiche Kommunikation zwischen einem Kundensystem und dem Wertübertragungszentrum nicht zu betrügerischen Zwecken nutzen (Replay-Attacke).

– Dritte oder Kunden können gegenüber dem Wertübertragungszentrum nicht die Verwendung eines ordnungsgemäßen Kundensystems durch ein manipuliertes Kundensystem vortäuschen. Spiegelt ein Dritter oder ein Kunde die Übertragung einer Zufallszahl und einer Safe-Box-ID vor, die nicht innerhalb eines Sicherungsmoduls erzeugt wurden, sondern ihm bekannt sind, so scheitert das Laden der Abrechnungsbeträge entweder an der separat durchgeführten Identifikation des rechtmäßigen Kunden durch Benutzername und Kennwort oder an der Kenntnis des privaten Schlüssels des Sicherungsmoduls, der dem Kunden unter keinen Umständen bekannt sein darf. (Deshalb ist der Initialisierungsprozess zur Schlüsselerzeugung in dem Sicherungsmodul und die Zertifizierung des öffentlichen Schlüssels durch den Kundensystemanbieter geeignet durchzuführen.)

– Dritte oder Kunden können nicht mit einem vorgetäuschten Wertübertragungszentrum gültige Abrechnungsbeträge in ein Kundensystem laden. Spiegelt ein Dritter oder ein Kunde die Funktionalität des Wertübertragungszentrums vor, so gelingt es diesem vorgeprägten Wertübertragungszentrum nicht, eine verschlüsselte Ladevorgangsidentifikationsnummer zu erzeugen, die im Briefzentrum ordnungsgemäß entschlüsselt werden kann. Zudem kann das Zertifikat des öffentlichen Schlüssels des Wertübertragungszentrums nicht gefälscht werden.

– Kunden können nicht unter Umgehung des Wertübertragungszentrums einen Freimachungsvermerk erstellen, dessen Ladevorgangsidentifikationsnummer derart verschlüsselt ist, dass sie im Briefzentrum als gültig entschlüsselt werden könnte.

[0042] Zur Erhöhung der Datensicherheit, insbesondere beim Suchen, ist eine unbegrenzte Anzahl von Zufallszahlen zur Hash-Wert-Bildung heranzuziehen.

– Die Länge der Zufallszahl ist daher möglichst groß und beträgt vorzugsweise mindestens 12 byte (96 bit). Die eingesetzte Sicherheitsarchitektur ist durch die Möglichkeit, kundenspezifische Schlüssel einzusetzen, ohne dass es notwendig ist, in zur Entschlüsselung bestimmten Stellen, insbesondere Briefzentren, Schlüssel bereit zu halten, den bekannten Verfahren überlegen. Diese vorteilhafte Ausgestaltung ist ein wesentlicher Unterschied zu den bekannten Systemen nach dem Information-Based Indicia Program (IBTP).

Vorteile der Sicherheitsarchitektur

[0043] Folgende Merkmale zeichnen die beschriebene Sicherheitsarchitektur gegenüber dem bekannten IBIP-Modell des US Postal Services der USA aus:

- Die eigentliche Sicherheit wird in den Systemen der Deutschen Post (Wertübertragungszentrum, Briefzentrum, Entgeltsicherungssystem) gewährleistet und liest damit vollständig im Einflussbereich der Deutschen Post.
- Es werden im Freimachungsvermerk keine Signaturen, sondern technisch gleichwertige und ebenso sichere (symmetrisch) verschlüsselte Daten und Hash-Werte angewandt. Hierzu wird im einfachsten Falle nur ein symmetrischer Schlüssel verwendet, der alleine im Einflussbereich der Deutschen Post liegt und somit leicht austauschbar ist.
- Im Briefzentrum ist eine Überprüfung aller Freimachungsmerkmale (nicht bloß Stichprobenweise) möglich.
- Das Sicherheitskonzept basiert auf einem einfachen, in sich geschlossenen Prüfkreislauf, der in Einklang mit einem hierauf angepassten Hintergrundsystem steht.
- Das System macht selbst ansonsten kaum feststellbare Dubletten erkennbar.
- Ungültige Phantasiemarken sind mit diesem Verfahren mit hoher Genauigkeit erkennbar.
- Neben der Plausibilitätsprüfung kann bei allen Freimachungsvermerken eine Überprüfung der Ladevorgangsidentifikationsnummer in Echtzeit erfolgen.

Sendungsarten

[0044] Mit der PC-Frankierung können alle Produkte des Versendungsdienstleisters wie beispielsweise "Brief national" (einschließlich Zusatzleistungen) und "Direkt Marketing national" gemäß einer vorhergehenden Festlegung durch den Versendungsdienstleister freigemacht werden.

[0045] Ein Einsatz für andere Versandformen wie Paket- und Expresssendungen ist gleichermaßen möglich.

[0046] Der Gebührenbetrag, der maximal über das Wertübertragungszentrum geladen werden kann, wird auf einen geeigneten Betrag festgelegt. Der Betrag kann je nach Anforderung des Kunden und dem Sicherheitsbedürfnis des Postdienstleisters gewählt werden. Während für einen Einsatz im Privatkundenbereich ein Gebührenbetrag von maximal mehreren hundert DM besonders zweckmäßig ist, werden für Einsätze bei Großkunden wesentlich höhere Gebührenbeträge vorgesehen. Ein Betrag in der Größenordnung

von etwa DM 500,- eignet sich sowohl für anspruchsvolle Privathaushalte als auch für Freiberufler und kleinere Unternehmen. Der in der Börse gespeicherte Wert sollte vorzugsweise den doppelten Wertbetrag systemtechnisch nicht überschreiten.

Falschfrankierte Sendungen

[0047] Falschfrankierte und nicht zur Beförderung geeignete, bereits bedruckte Schreiben, Umschläge etc. mit einem gültigen Freimachungsvermerk werden dem Kunden gutgeschrieben.

[0048] Durch geeignete Maßnahmen, beispielsweise durch eine Stempelung von in dem Briefzentrum eingehenden Sendungen, ist es möglich festzustellen, ob eine Sendung bereits befördert wurde. Hierdurch wird verhindert, dass Kunden bereits beförderte Sendungen vom Empfänger zurück erhalten und diese zur Gutschrift bei dem Postdienstbetreiber, beispielsweise der Deutschen Post AG, einreichen.

[0049] Die Rücksendung an eine zentrale Stelle des Versendungsdienstleisters, beispielsweise der Deutschen Post, ermöglicht ein hohes Maß an Entgeltsicherung durch Abgleich der Daten mit Abrechnungsbeträgen und die Kenntnis über die häufigsten Zusendungsgründe. Hierdurch besteht gegebenenfalls die Möglichkeit der Nachsteuerung durch Änderung der Einführungs Voraussetzungen mit dem Ziel der Reduzierung der Rücksendequote.

Gültigkeit von Freimachungswerten

[0050] Vom Kunden gekaufte Abrechnungswerte sind aus Gründen der Entgeltsicherung beispielsweise nur 3 Monate gültig. Ein entsprechender Hinweis ist in der Vereinbarung mit dem Kunden aufzunehmen. Können Frankierwerte nicht innerhalb von 3 Monaten aufgebraucht werden, muss vom Kundensystem die Kontaktierung des Wertübertragungszentrums zu einer erneuten Herstellung von Freimachungsvermerken aufgenommen werden. Bei dieser Kontaktierung wird, wie beim ordentlichen Laden von Abrechnungsbeträgen, der Restbetrag eines alten Abrechnungsbetrages einem neu ausgegebenen Abrechnungsbetrag zugeschlagen und unter einer neuen Ladevorgangsidentifikationsnummer dem Kunden zur Verfügung gestellt.

Besondere betriebliche Behandlung

[0051] Grundsätzlich können die Freimachungsvermerke eine beliebige Form aufweisen, in der die in ihnen enthaltenen Informationen wiedergegeben werden können. Es ist jedoch zweckmäßig, die Freimachungsvermerke so zu gestalten, dass sie wenigstens bereichsweise die Form von Barcodes aufweisen. Bei der dargestellten Lösung des 2D-Barcodes und der daraus resultierenden Entgeltsicherung sind folgende Besonderheiten in der Produktion zu berücksichtigen: PC-frankierte Sendungen können über alle Einlieferungs-möglichkeiten, auch über Briefkasten, eingeliefert werden.

[0052] Durch die Festlegung von Zulassungsvoraussetzungen für Hersteller von für die Schnittstellen relevanten Bestandteilen des Frankierungssystems, insbesondere für Hersteller und/oder Betreiber von Kundensystemen, wird die Einhaltung der dargestellten Sicherheitsmaßnahmen weiter erhöht.

Übergeordnete Normen, Standards und Vorgaben

International Postage Meter Approval Requirements (IPMAR)

[0053] Vorzugsweise finden die Vorschriften der aktuellen Fassung des Dokuments International Postage Meter Approval Requirements (IPMAR), UPU S-30, ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die weitestmögliche Einhaltung aller dort genannten "Requirements" ist für das Kundensystem sinnvoll.

Digital Postage Marks: Applications, Security & Design

[0054] Grundsätzlich finden die Vorschriften der aktuellen Fassung des Dokuments Digital Postage Marks: Applications, Security & Design (UPU: Technical Standards Manual) ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die Einhaltung des "normativen" Inhalts sowie die weitestgehende Beachtung des "informativen" Inhalts dieses Dokuments ist für das Kundensystem sinnvoll.

[0055] Vorzugsweise finden über die übergeordneten Normen und Standards hinaus Regelungen und Bestimmungen des jeweiligen Versendungsdienstleistungsunternehmens gleichfalls Anwendung.

[0056] Durch eine Zulassung lediglich solcher Systeme, die alle gesetzlichen Bestimmungen ebenso erfüllen wie alle Normen und Standards des Versendungsdienstleisters, werden Datensicherheit und Zuverlässigkeit des Systems ebenso gewährleistet wie seine Benutzerfreundlichkeit.

Weitere Gesetze, Verordnungen, Richtlinien, Vorschriften, Normen und Standards

[0057] Grundsätzlich finden alle Gesetze, Verordnungen, Richtlinien, Vorschriften, Normen und Standards der jeweils gültigen Fassung Anwendung, die zur Entwicklung und zum Betrieb eines technischen Kundensystems in der konkreten Ausprägung zu beachten sind.

Systemtechnische Interoperabilität

[0058] Die systemtechnische Interoperabilität bezieht sich auf die Funktionsfähigkeit der Schnittstellen des Kundensystems, beziehungsweise auf die Einhaltung der in den Schnittstellenbeschreibungen spezifizierten Vorgaben.

Schnittstelle, Abrechnungsbetrag, Kommunikationsweg, Protokolle

[0059] Die Kommunikation über die Schnittstelle Abrechnungsbetrag erfolgt vorzugsweise über das öffentliche Internet auf der Basis der Protokolle TCP/IP und HTTP. Der Datenaustausch kann optional per HTTP über SSL verschlüsselt werden (https). Hier dargestellt ist der Soll-Prozess einer erforderlichen Übertragung.

[0060] Der Datenaustausch erfolgt vorzugsweise, sofern möglich, über HTML- und XML-kodierte Dateien. Die textlichen und graphischen Inhalte der HTML-Seiten sind im Kundensystem darzustellen.

[0061] Es erscheint empfehlenswert, bei den Kommunikationsseiten auf eine bewährte HTML-Version zurückzugreifen und auf die Verwendung von Frames, eingebetteten Objekten (Applets, Activex etc.) und ggf. animierten GIFs zu verzichten.

Anmeldung zum Laden eines Abrechnungsbetrages (erste Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum)

5 [0062] Im Rahmen der ersten Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum werden das Zertifikat des Sicherungsmoduls sowie ein Aktionsindikator A unverschlüsselt und unsigniert übertragen.

10 Rückmeldung zur Anmeldung (erste Antwort vom Wertübertragungszentrum zum Sicherungsmodul)

[0063] Die Rückmeldung des Wertübertragungszentrums enthält das eigene Zertifikat des Wertübertragungszentrums, einen verschlüsselten Sitzungsschlüssel und die digitale Signatur des verschlüsselten Sitzungsschlüssels.

Zweite Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

20 [0064] Im Rahmen dieser Übertragung sendet das Sicherungsmodul den neu verschlüsselten Sitzungsschlüssel, die verschlüsselte Zufallszahl und den verschlüsselten Datensatz mit Nutzdaten (Höhe eines vorab geladenen Abrechnungsbetrages, Restwert des aktuellen Abrechnungsbetrages, aufsteigendes Register aller Abrechnungsbeträge, die letzte Ladevorgangsidentifikationsnummer – (alles asymmetrisch mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt). Gleichzeitig sendet das Sicherungsmodul die digitale Signatur dieser verschlüsselten Daten. Im gleichen Zeitraum kann das Kundensystem weitere, nicht verschlüsselte und nicht signierte Nutzungsprotokolle oder Nutzungsprofile an das Wertübertragungszentrum senden.

35 [0065] Es ist zweckmässig, dass die Nutzungsdaten in ein Nutzungsprotokoll eingetragen werden und dass das Nutzungsprotokoll und/oder die darin vermerkten Einträge digital signiert werden.

40 Zweite Antwort vom Wertübertragungszentrum zu dem Sicherungsmodul

[0066] Das Wertübertragungszentrum übermittelt die symmetrisch verschlüsselte Zufallszahl und die symmetrisch verschlüsselte Ladevorgangsidentifikationsnummer an das Sicherungsmodul. Außerdem übermittelt das Wertübertragungszentrum die mit dem öffentlichen Schlüssel des Sicherungsmoduls erstellte Ladevorgangsidentifikationsnummer, Login-Informationen für das Sicherungsmodul sowie einen neuen Sitzungsschlüssel an das Sicherungsmodul. Die gesamten übertragenen Daten werden zudem digital signiert.

Dritte Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

[0067] Im Rahmen der dritten Übertragung werden von dem Sicherungsmodul der neue Sitzungsschlüssel, die neue Ladevorgangsidentifikationsnummer zusammen mit Nutzdaten zur Bestätigung der erfolgreichen Kommunikation allesamt in verschlüsselter und digital signierter Form an das Wertübertragungszentrum übertragen.

Dritte Antwort vom Wertübertragungszentrum an das Sicherungsmodul

[0068] Bei der dritten Antwort quittiert das Wertübertragungszentrum den Erfolg der Übertragung ohne Anwen-

dung kryptographischer Verfahren.

Deinstallation

[0069] Die Möglichkeit einer Deinstallation des Kundensystems muss durch den Kunden möglich sein.

[0070] Die detaillierte, technische Beschreibung der Schnittstelle Abrechnungsbetrag erfolgt mit Konzeption des posteigenen Wertübertragungszentrums.

Nutzungsprotokoll und Nutzungsprofil

[0071] Im Kundensystem ist im Rahmen jeder Erzeugung eines Freimachungsvermerks ein Protokolleintrag zu erzeugen, der alle Angaben des jeweiligen Freimachungsvermerks – versehen mit einer digitalen Signatur des Sicherungsmoduls – enthalten muss. Weiterhin muss im Protokoll jeder Fehlerstatus des Sicherungsmoduls derart verzeichnet werden, dass die manuelle Löschung dieses Eintrags bei der Überprüfung bemerkt wird.

[0072] Das Nutzungsprofil enthält eine aufbereitete Zusammenfassung der Nutzungsdaten seit der letzten Kommunikation mit dem Wertübertragungszentrum.

[0073] Ist ein Kundensystem in eine beim Kunden befindliche und eine zentral (z. B. im Internet befindliche) Komponente aufgeteilt, so muss das Nutzungsprofil in der zentralen Komponente geführt werden.

Schnittstelle, Freimachungsvermerk, Bestandteile und Ausprägungen

[0074] Das Kundensystem muss in der Lage sein, PC-Freimachungsvermerke zu erzeugen, die exakt den Vorgaben der Deutschen Post, beziehungsweise dem Rahmen der gängigen CEN- und UPU-Standards entsprechen.

[0075] PC-Freimachungsvermerke bestehen vorzugsweise aus folgenden drei Elementen:

- Einem 2-dimensionalen Strichcode, Barcode oder Matrixcode, in dem sendungsspezifische Informationen in maschinenlesbarer Form dargestellt sind. (Zweck: Automatisierung in der Produktion und Entgeltsicherung der Deutschen Post.)
- Text in Klarschrift, der wichtige Teile der Strichcode-Information in lesbarer Form wiedergibt. (Zweck: Kontrollmöglichkeit für den Kunden sowie in der Produktion und Entgeltsicherung der Deutschen Post.)
- Eine den Versandungsdienstleister, beispielsweise die Deutsche Post, kennzeichnende Marke wie beispielsweise ein Posthorn.

Spezifikation des Dateninhaltes

[0076] Zweckmäßigerweise enthalten Strichcode und Klartext des PC-Freimachungsvermerks folgende Informationen:

Tabelle

Inhalt des PC-Freimachungsvermerks

[0077] Beschrieben wird hier nur der Inhalt des Freimachungsvermerks. Die Vorschriften des Versandungsdienstleisters für den Inhalt der Adressangaben behalten unverändert ihre Gültigkeit.

Spezifikation der physikalischen Ausprägung auf Papier(Layout)

[0078] Der Freimachungsvermerk ist vorteilhafterweise im Anschriftenfeld linksbündig oberhalb der Anschrift auf der Sendung angebracht.

[0079] Das Anschriftenfeld wird in der jeweils gültigen Fassung der Normen des Versandungsdienstleisters spezifiziert. So werden insbesondere folgende Freimachungen ermöglicht:

- Aufdruck auf den Briefumschlag,
- Aufdruck auf Klebeetiketten oder
- Verwendung von Fensterbriefumschlägen derart, dass der Aufdruck auf den Brief durch das Fenster vollständig sichtbar ist.

[0080] Für die einzelnen Elemente des Freimachungsvermerks gilt vorzugsweise:

- Verwendet wird zunächst der Strichcode vom Type Data Matrix, dessen einzelne Bildpunkte eine Kantenlänge von mindestens 0,5 Millimeter aufweisen sollten. Im Hinblick auf lesetechnische Voraussetzungen sollte ein 2D-Barcode in Form der Data Matrix mit einer minimalen Pixelgröße von 0,5 mm bevorzugt zur Anwendung kommen. Eine ggf. zweckmäßige Option besteht darin, die Pixel-Größe auf 0,3 mm zu reduzieren. Bei einer Darstellungsgröße von 0,5 mm pro Pixel ergibt sich eine Kantenlänge des gesamten Barcodes von ca. 18 bis 20 mm, wenn alle Daten wie beschrieben eingehen. Falls es gelingt, Barcodes mit einer Pixelgröße von 0,3 mm in der ALM zu lesen, lässt sich die Kantenlänge auf ca. 13 mm reduzieren. Eine nachträgliche Erweiterung der Spezifikationen auf die Verwendung eines anderen Barcodes (z. B. Aztec) bei gleichen Dateninhalten ist möglich.

[0081] Eine bevorzugte Ausführungsform des Layouts und der Positionierung der einzelnen Elemente des Freimachungsvermerks ist nachfolgend in Fig. 5 beispielhaft dargestellt.

[0082] Die "kritischste" Größe ist die Höhe des dargestellten Fensters eines Fensterbriefumschlags mit einer Größe von 45 mm × 90 mm. Hier dargestellt wird ein DataMatrix-Code mit einer Kantenlänge von ca. 13 mm, der bei Verwendung der vorgeschlagenen Datenfelder nur bei einer Pixelauflösung von 0,3 mm möglich ist. Ein Code mit einer Kantenlänge von 24 mm lässt bezüglich der zur Verfügung stehenden Höhe keinen ausreichenden Raum für Angaben zur Anschrift.

Druckqualität und Lesbarkeit

[0083] Verantwortlich für den einwandfreien Aufdruck des Freimachungsvermerks sind der Hersteller des Kundensystems im Rahmendes Zulassungsverfahrens sowie der Kunde im späteren Betrieb. Hierzu ist der Kunde durch geeignete Hinweise in einem Benutzerhandbuch und einem Hilfesystem hinzuweisen. Dies gilt insbesondere für das saubere Haften von Etiketten und das Verhindern des Verrutschens (von Teilen) des Freimachungsvermerks außerhalb des sichtbaren Bereichs von Fensterbriefumschlägen.

[0084] Die maschinelle Lesbarkeit von Freimachungsvermerken steht in Abhängigkeit von der verwendeten Druckauflösung und vom Kontrast. Sollen statt schwarz auch andere Farben zur Anwendung kommen, so ist mit einer geringeren Leserate zu rechnen. Es ist davon auszugehen, dass

die geforderte Leserate bei einer im Drucker verwendeten Auflösung von 300 dpi ("dots der inch") bei hohem Druck-Kontrast gewährleistet werden kann; das entspricht etwa 120 Bildpunkten pro Zentimeter.

Testdrucke

5

[0085] Das Kundensystem muss in der Lage sein, Freimachungsvermerke zu produzieren, die in Ausprägung und Größe gültigen Freimachungsvermerken entsprechen, jedoch nicht für den Versand bestimmt sind, sondern für Kontrollausdrucke und der Drucker-Feinjustierung dienen. 10

[0086] Vorzugsweise ist das Kundensystem so gestaltet, dass die Testdrucke sich in einer für das Versendungsunternehmen erkennbaren Weise von tatsächlichen Freimachungsvermerken unterscheiden. Dazu wird beispielsweise in der Mitte des Freimachungsvermerks die Aufschrift "MUSTER – nicht versenden" angebracht. Mindestens zwei Drittel des Barcodes, sollen durch die Aufschrift oder anderweitig unkenntlich gemacht werden. 15 20

[0087] Neben echten (bezahlten) Freimachungsvermerken dürfen außer gesondert gekennzeichneten Testdrucken keine Nulldrucke hergestellt werden.

Anforderungen an das Kundensystem

25

Basis-System

Überblick und Funktionalität

30

[0088] Das Basis-System dient als Bindeglied zwischen den anderen Komponenten der PC-Frankierung, namentlich dem Wertübertragungszentrum, des Sicherungsmoduls, dem Drucker und dem Kunden. Es besteht aus einem oder mehreren Computersystemen, zum Beispiel PCs, die ggf. auch durch ein Netzwerk miteinander verbunden sein können. 35

[0089] Die Erfindung ermöglicht es, bei verschiedenen Schritten der Erzeugung von Freimachungsvermerken den weiteren Vorgang der Berechnung eines Gebührenbetrages zu unterbrechen. 40

Patentansprüche

1. Verfahren zum Versehen von Postsendungen mit Frankierungsvermerken, wobei ein Kundensystem ein Drucken von Frankierungsvermerken auf Postsendungen steuert, **dadurch gekennzeichnet**, dass in einer Datei erfasst wird, für welche durch einen Druckbefehl erzeugte Frankiervermerke keine Versendung einer Postsendung erfolgt. 45 50

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Informationen der Datei in ein Gebühren-erstattungsformular übernommen werden.

3. Verfahren nach einem oder beiden der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass die Datei und/oder das Gebührenerstattungsformular an eine Erstattungsstelle übermittelt werden. 55

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die Übermittlung an einen Server erfolgt und dass das Kundensystem Identifikationsdaten über die nicht zu versendenden Sendungen an den Server übermittelt, und dass der Server die Identifikationsdaten an wenigstens eine Überprüfungsstelle weiterleitet. 60

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die Übermittlung durch eine e-mail erfolgt. 65

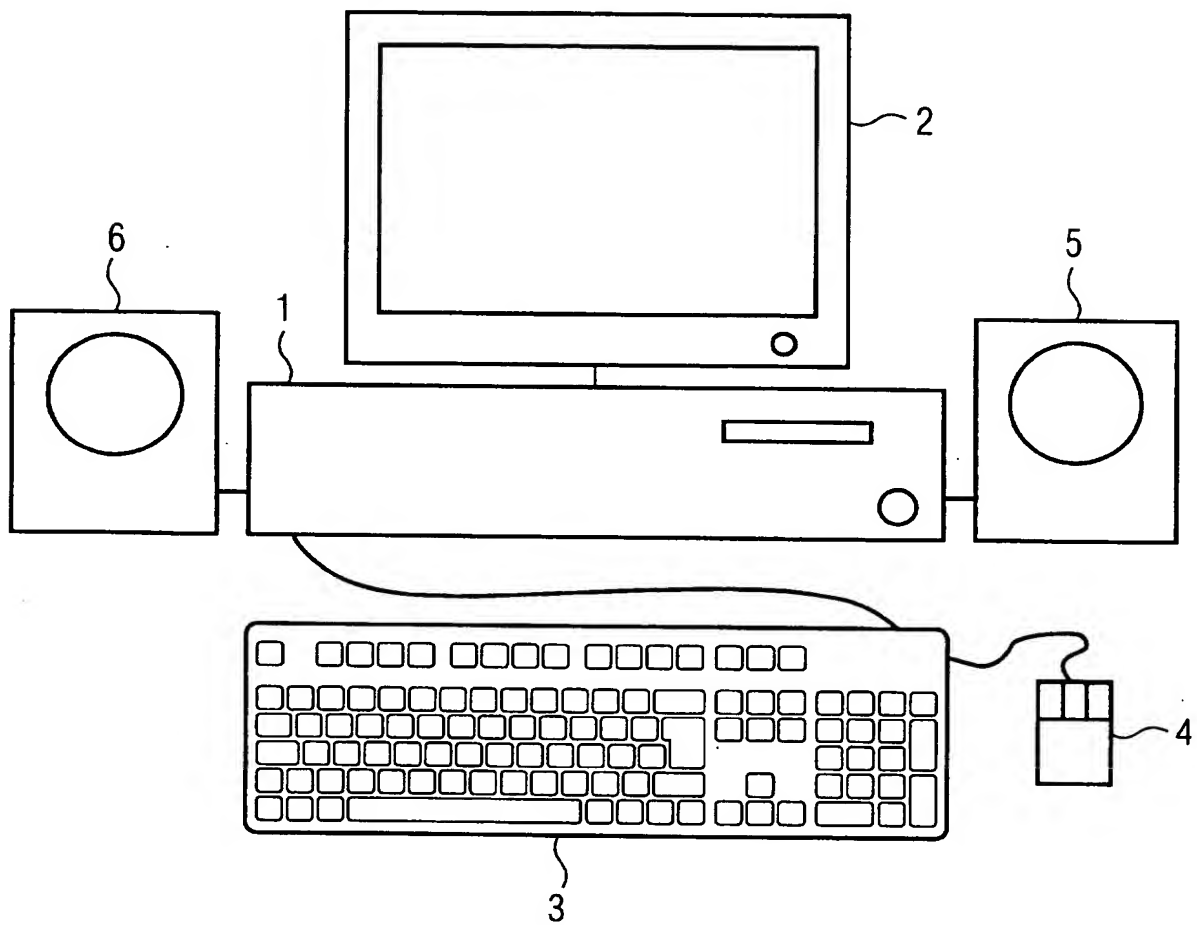
6. Verfahren nach einem oder beiden der Ansprüche 3 oder 4, dadurch gekennzeichnet, dass die Übermittlung

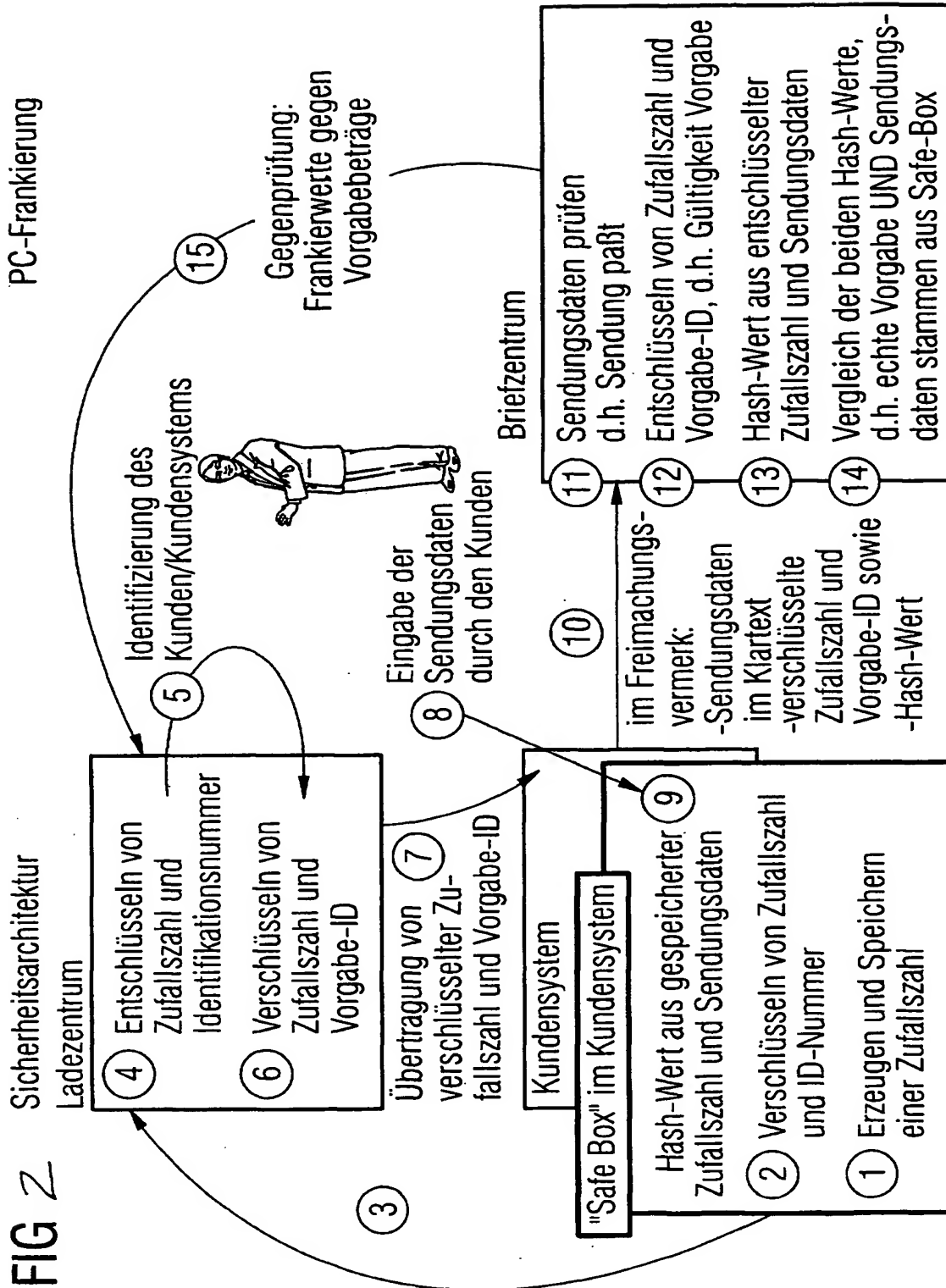
an eine Webseite erfolgt.

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

FIG 1





Maskenausschnitt

FIG. 3

Journal

Kunden-ID 1234567890
Rechtsanwaltsbüro Schulte + Müller, Bonn

Guthaben 78,56 EUR
gültig bis 30.11.00

Datum/Uhrzeit	Name	Anschrift	PLZ/Ort	Sendung	Porto EUR	Hinweis	Nicht abgesandt
06.11.00 11:23	Müller KG	Schlosserstr. 10	60323 Frankfurt	Standardbrief	0,56	Müller	<input type="checkbox"/>
06.11.00 11:24	Schreiner GmbH	Hauptstr. 12	60321 Frankfurt	Kompakbrief	1,12	Schulte	<input checked="" type="checkbox"/> Stormo
06.11.00 11:24	Schreiner GmbH	Hauptstr. 12	60321 Frankfurt	Standardbrief	0,56	Schulte	<input type="checkbox"/>
06.11.00 11:26	Bernhard Lang	Landauer Str. 10	60276 Frankfurt	Standardbrief	0,56		<input type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>

Hinweis: Es werden nur die Sendungen angezeigt, die auf diesem PC erstellt wurden.